CLAIMS IN THE CASE

Please amend Claims 1, 4, 10, 20 and 23, as presented below.

1. (Currently amended) A method for managing access to a network, comprising:

providing wireless communication in a network;

~~providing a firewall protection between said network and a wireless access device;~~

submitting an identification code to said network from said wireless access device, said identification code a media control number associated with and pertaining to said wireless access device;

determining the validity of said identification code;

granting wireless network access to said wireless access device when said identification code is valid;

denying wireless network access to said wireless access device when said identification code is not valid;

issuing an alert when said identification code is not valid.

2. (Original) The method described in Claim 1, wherein said providing said wireless communication is accomplished with an intelligent concentrator enabled for wireless communication.

3. (Original) The method described in Claim 2, wherein said providing said wireless communication is accomplished in circuitry resident in said intelligent concentrator.

4. (Currently amended) The method described in Claim 2, wherein said media control number ~~identification code~~ is a media access control number of said wireless device.

5. (Original) The method described in Claim 1, wherein said determining said validity of said identification code is accomplished by reference to a list of valid identification codes.

~~6. (Previously presented) The method described in Claim 2, wherein said list of valid~~ identification codes is resident in said intelligent concentrator.

7. (Original) The method described in Claim 5, wherein said list of valid identification codes is resident in a server in said network.

8. (Original) The method described in Claim 1, wherein said denying said wireless access to said network is accomplished simultaneously with granting access to said wireless accesses devices with valid identification codes.

9. (Original) The method described in Claim 1, wherein said network is a wireless personal area network.

10. (Currently amended) A computer network, comprising:

a server;

a wireless connection device communicatively coupled with said server;

a wireless access device enabled to wirelessly submit an identification code to said wireless connection device, said identification code a media access control number associated with and pertaining to said wireless access device; and

a firewall communicatively coupled to said server and said wireless connection device, wherein said firewall is enabled to grant network access to said wireless access device when said identification code is valid and to deny access to said network by said wireless access device and issue an alert when said identification code is not valid.

11. (Original) The computer network described in Claim 10, wherein said server is an internet portal.

12. (Original) The computer network described in Claim 10, wherein said wireless connection device is an intelligent concentrator enabled for wireless communication.

13. (Original) The computer network described in Claim 10, wherein said wireless access device is a wirelessly enabled laptop computer.

14. (Original) The computer network described in Claim 10, wherein said wireless access device is a wirelessly enabled personal data assistant.

15. (Original) The computer network described in Claim 10, wherein said wireless access device is a wireless telephone enabled for data communication.

16. (Original) The computer network described in Claim 10, wherein said wireless access device is a wirelessly enabled computer peripheral device.

17. (Previously presented) The computer network described in Claim 12 wherein said firewall is a distributed firewall and is resident in said intelligent concentrator.

---

18. (Original) The computer network described in Claim 17, wherein said distributed firewall is enabled to obtain a list of valid identification codes from said server.

19. (Original) The computer network described in Claim 18, wherein said distributed firewall is enabled to verity the validity of said identification code submitted from a wireless access device.

20. (Currently amended) An intelligent concentrator, comprising:

a housing;

a cable connector coupled to said housing and adapted to communicatively couple said intelligent concentrator to a network data cable;

electronic circuitry mounted in said housing enabled to wirelessly communicate with a wireless access device and a network; and

a distributed firewall resident in said electronic circuitry wherein said firewall is enabled to control the access to said network of said wireless access device, said control via a validated identification code transmitted from said wireless access device, said identification code a media control number associated with and pertaining to said wireless access device .

21. (Original) The intelligent concentrator described in Claim 20, wherein said intelligent concentrator is enabled as a hub of a personal area network.

22. (Original) The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to obtain a list of valid identification codes from a server in said network.

23. (Currently amended) The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to verify validity of said identification code submitted by said wireless access device, said media control number a media access control number..

24. (Original) The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to deny access to said wireless access device if said identification code is not valid.

25. (Original) The intelligent concentrator described in Claim 20, wherein said distributed firewall is enabled to issue an alarm to a network manager is said identification code is not valid.